COMMENTARY
JUNE 2022

NON STATE ACTORS IN CYBERSPACE: AN ATTEMPT TO A TAXONOMIC CLASSIFICATION, ROLE, IMPACT AND RELATIONS WITH A STATE'S SOCIO-ECONOMIC STRUCTURE

PIERLUIGI PAGANINI

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

NON STATE ACTORS IN CYBERSPACE: AN ATTEMPT TO A TAXONOMIC CLASSIFICATION, ROLE, IMPACT AND RELATIONS WITH A STATE'S SOCIO-ECONOMIC STRUCTURE

Pierluigi Paganini

UNIVERSITÀ DEGLI STUDI FIRENZE

Commentary

June 2022

ABOUT THE AUTHOR

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

NON STATE ACTORS IN CYBERSPACE: AN ATTEMPT TO A TAXONOMIC CLASSIFICATION, ROLE, IMPACT AND RELATIONS WITH A STATE'S SOCIO-ECONOMIC STRUCTURE

Introduction

Cyber Non-State Actors (CNSA) are key figures in our globalized world: their operations could have a significant impact on international affairs, politics, and on the economy, as much as states do.

Non-state actors include multinational corporations, collectives of hacktivists, non-governmental organizations (NGOs), cybercrime syndicates, private military organizations, media outlets, terrorist groups, labor unions, organized ethnic groups, lobby groups, criminal organizations, private businesses, and others.

CNSA can operate with different aims: some are financially motivated, like cybercrime gangs, while others are politically motivated, like state-sponsored hackers and hacktivists.

The capability of Cyber Non-State Actors to influence state decision-making processes depends on their specific category.

The role of CNSA is crucial, due to the growing importance of cyberspace to modern society.

Cyberspace is a domain without borders, where businesses operate while nation-state actors conduct their activities. Some of those activities being malicious.

The number of cyber-attacks continues to increase as well as their level of sophistication. For this reason, the behavior of each actor in the cyber arena is becoming a national security concern for every government. The asymmetric nature of the cyber-attacks, the problem of attribution, the adoption of different legal frameworks by states, the low barriers to entry make the cyberspace an attractive arena for both nation-state actors and CNSA.

Unfortunately, ever more often, we are observing a growing number of actors that are using cyber tools in warfare, cyber weapons that could allow attackers to achieve same results of a conventional weapon, while making attribution hard.

The current conflict between Russia and Ukraine is characterized by the presence of multiple Cyber Non-State Actors, but this isn't the first time that states have faced with offensives launched by this category of attacks.

Looking back at 2007, Estonia fell victim to a powerful cyber-attack that shut down government services, telecommunications, and banks in the country. The attack was launched in response to the Estonian government's removal of a Soviet war monument from downtown Tallinn. It was a massive distributed denial of service attack (DDoS), apparently launched by patriotic Russian hackers and cybercriminals.

The involvement of CNSA make it hard to attribute the attack to Russia and impossible to sanction Moscow. The attack was organized to appear as independently orchestrated by different threat actors without an evident link with Moscow. It was launched with sabotage purpose along with a psychological effect on the targeted population.

Some CNSA are therefore unofficial emanation of the States where most of their components are located and act as 'corsairs' for their country, often conducting activities aimed at: a) extorting and stealing money; b) attacking enemy countries institutions and infrastructures; c) cyber-espionage.

In fact, several states tolerate or even protect CSNA in order to: a) create the conditions for development and prosperity of as many cyber-operators with hacking capabilities as possible (we will approach this specific topic further within this paper), b) to be able to get access to information and intelligence of different kind.

Classification of CNSA

Cyber Non-state actors could be classified according to different axis of analysis, such as their motivation, their form of organization, and their relationship with the host state.

CNSA could be financially motivated, support the cyber strategy of a government by providing it with profits generated by their malicious activities, or they can conduct their operations for political or ideological reasons.

Some CNSA actors operate directly, but unofficially, under the control of the host state, its intelligence and military agencies, while others provide their support to state actors for money or in exchange of any sort of advantage: for example, the immunity for their criminal activities conducted against foreign entities. Other CNSA act in open contrast with any government for ideological or religious purposes: this is the case of terrorist organizations that conduct cyber operations against subjects (states, economic entities or private citizens) that are considered infidels.

Cybercrime syndicates

Cybercrime organizations are probably the most active entities in the threat landscape: analysists estimate cybercrime to be world's third-largest economy after the U.S. and China.

Cybercrime was estimated[1] to cost global economy $10.5 Trillion annually by 2025, according to the Internet Crime Report (IC3) 2020[2] released in 2021. In 2020 the reported losses exceeded $4.2 billion, and authorities observed an increase of more than 300,000 complaints from 2019 (+69%).

1 Steve Morgan, Cybersecurity Ventures (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025 - https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2 FBI IC3 (2021). Internet Crime Report 2020 - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Figure 1 - Source CyberSecurity Ventures

The single factor that most of all has contributed to such significant increase is the rapid evolution of the cybercrime-as-a-service (CaaS) model in the threat landscape.

Cybercrime operations could cause damage and destruction of data and infrastructures, theft of money and intellectual property, and theft of personal and financial data. In many cases there is a thin line between cybercrime organizations and Advanced Persistent Threat groups that operate on behalf of states. Moreover, cybercrime organizations have generally a higher level of organizational structure and in some cases strong relationships with the host state. Just like in other cases, such host states can involve them in cyber operations, leveraging on their financial interests and using them as mercenaries, but they can also force these groups to collaborate by promising them some sort of immunity.

The main advantage of involving cybercriminal organizations in nation-state operation is to make quite difficult if not impossible the attribution to state that recruited them. Criminal organizations may provide knowledge, manpower and attack infrastructures in a cyber scenario. Thanks to the Cybercrime-as-a-Service (Caas) model, nation-state actors

could therefore quickly carry our hit-and-run operations, still remaining 'under the radar'.

Looking at the past, one of the most powerful cybercriminal organizations ever, the Russian Business Network, is believed to have to have contributed to cyber operations against Georgia during the conflict that took place in 2008.

Back to nowadays, criminal organizations like the Conti and Stormous gangs have announced their support to Russia, ahead of the current invasion of Ukraine. The involvement such cybercrime organizations like the Conti group in a cyber conflict represents a serious threat for organizations on a global scale. These threat actors could operate under the control of the Russian government, but it will be really difficult to demonstrate this link and sanction Moscow in case of attacks against critical infrastructure of EU and NATO countries. The capabilities and the information gathered by cybercrime organizations could also be exploited in future attacks orchestrated by state-sponsored hackers.

Hacktivists and Patriotic hackers

Online activists, also known as hacktivists, are independent hackers that are politically or ideologically motivated. Hacktivits could act as lone wolves or within decentralized, transnational collectives like Anonymous. These collectives are often constellations of groups that could operate in temporary aggregations, depending on specific operations that are launched and orchestrated through social media platforms and hacking forums. Unlike cybercrime syndicates these group lack a formalized internal structure.

Patriotic hacker groups, unlike hacktivists, are exclusively driven by a patriotic devotion and their cyber operations aims at defending the interests of their state. In some cases, these groups have close collaborations with the states they defend and could also be involved in attacks aimed at infrastructure of organizations and foreign states.

Cyber Mercenaries

Cyber mercenaries are IT experts and hackers that may be hired to conduct cyber operations, even hybrid warfare operations and packed together within ad-hoc CNAS. They can provide attack infrastructures, knowledge on targets, exploits codes, and support to hacking attacks.

These professionals could operate in groups, they often belong to prolific hacking communities that allow them to rapidly recruit other mercenaries or to acquire data and software, even malware, that could be used in cyber-attacks.

The capabilities of such groups have rapidly increased in recent years also thanks to the diffusion of automated attack tools. The role of these experts is essential in hit-and-run operations aimed at gathering intelligence to conduct diversionary attacks while nation-state actors launch their offensive against the real target.

Mercenaries, especially single individuals, could provide support for military operations in the form of defensive security and training to member of state cyber army. The UN Working Group on the use of mercenaries has classified cyber mercenaries as a specific category of actors that can generate mercenary-related activities.

Their involvement in a cyber warfare context can result in the disruption and damaging of military or civilian infrastructure and services, and also cause serious human harm.

CNSA and Nation state actors in modern conflict

The ongoing conflict in Ukraine was characterized by an intense activity only, threat actors were involved in sabotage, propaganda, and cyber espionage campaigns. The analysis of the cyber arena is very complex due to the presence of both nation-state actors and CNSA as reported in the following table.

GROUP	SUPPORTS	TYPE	COMMS	LOC	GROUP	SUPPORT	TYPE	COMMS	LOC
Anonymous Associated					Pro-Ukraine Groups				
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia	BlueHornetAPT49 (ATW)	Ukraine	Hack	Twitter	UNK
LiteMods	Ukraine	Psyops/DDoS	Twitter	UNK	KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK
SHDWSec	Ukraine	Hackivism	Twitter	UNK	GNG	Ukraine	DDoS	Twitter	Georgia
N3UR0515	Ukraine	DDoS	Twitter	UNK	Spot	Ukraine	DDoS	Twitter	UNK
PuckArks	Ukraine	Pysops	Twitter	UNK	GhostClan	Ukraine	DDoS/Hack	Telegram	UNK
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia	1LevelCrew	Ukraine	DDoS	Twitter	UNK
YourAnonNews	Ukraine	Psyops	Twitter	UNK	Hydra UG	Ukraine	Radio	Twitter	UNK
DeepNetAnon	Ukraine	Radio/hack	Twitter	UNK	SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK
Anonymous Younes	Ukraine	DDoS/Hack	Twitter	UNK	Ring3API	Ukraine	Hack	Twitter	Ukraine
0xAnonLeet	Ukraine	DDoS/hack	Twitter	UNK	Belarusian Cyber-Partisans	Ukraine	Ransomware	Twitter	Belarus
AnonGh0st	Ukraine	DDoS/Hack	Twitter	UNK	NB65	Ukraine	Ransomware	Twitter	UNK
Anonymous Romania	Ukraine	DDoS/Hack	Twitter	Romania	Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey
Shadow_Xor	Ukraine	Databreach	Twitter	UNK	Shadow_Xor	Ukraine	UNK	Twitter	UNK
PuckArks	Ukraine	Defacement	Twitter	UNK	The Connections	Ukraine	UNK	Twitter	UNK
Squad303	Ukraine	DDoS/SMS	Twitter	Poland	Rabbit Two	Ukraine	Hack/DDoS	Twitter	UNK
Synthynt	Ukraine	Ransomware	Twitter	UNK	SecDet	Ukraine	Hack	Twitter	US
GhostSec	Ukraine	Hack	Telegram	UNK	BeeHive Cybersecurity	Ukraine	Phishing/hack	Twitter	UNK
DDoS Secrets	Ukraine	Databreach	Twitter	UNK	Cyber_legion_hackers	Ukraine	Deface/DDoS	Twitter	UNK
v0g3lSec	Ukraine	Hack	Twitter	UNK	Stand for Ukraine	Ukraine	hack/ DDoS	UNK	Ukraine
Anonymous News	Ukraine	DDoS	Twitter	UNK	BrazenEagle (ATW)	Ukraine	Hack	Telegram	UNK
DoomSec	Ukraine	DDoS/Hack	Twitter	UNK	Bandera Hackers	Ukraine	Hack/DDoS	Twitter	UNK
CyberNinja Security Team	Ukraine	Hack	Twitter	UNK	HackenClub	Ukraine	DDoS/hack	Twitter	Ukraine
ReaperSec NEW	Ukraine	Hack/DDoS	Twitter	UNK	Pro-Russia Groups				
HAL9000 NEW	Ukraine	Hack/DDoS	Twitter	UNK	RedBanditsRU	Russia	Hack	Twitter	Russia
RedCult NEW	Ukraine	Hack/DDoS	Twitter	UNK	Stormous Ransomware	Russia	Ransomware	Telegram	UNK
Nation-State					Hydra	Russia	Dox/DDoS	Twitter	Russia
GhostWriter UNC1151	Russia	Hack	UNK	Belarus	RaHDit	Russia	Hack	UNk	Russia
SandWorm	Russia	Hack	UNK	Russia	Xaknet	Russia	Hack	Site	Russia
Gamaredon	Russia	Hack	UNK	Russia	Killnet	Russia	Hack/DDoS	Telegram	Russia
DEV-0586 APT	Russia	Hack	UNK	Russia	404 Cyber Defense	Russia	DDoS	Twitter	UNK
DEV-0665 APT	Russia	Hack	UNK	Russia	WeretheGoons	Russia	Hack	Twitter	Russia
FancyBear APT	Russia	Hack	UNK	Russia	punisher_346	Russia	PsyOps	Twitter	UNK
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine	Lorec53	Russia	Hack	UNK	Russia
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine	DDoS Hacktivist Team	Russia	DDoS	Telegram	Russia
Internet Forces of Ukraine	Ukraine	Pysops	UNK	Ukraine	cyberwar_world	Russia	Hack/ddos	Telegram	Russia
MustangPanda APT	UNK	Hack	UNK	China	Zsecnet NEW	Russia	Hack/DDoS	Telegram	Russia
Curious George	UNK	Hack	UNK	China	DivisionZ NEW	Russia	Hack/DDoS	Telegram	Russia

Figure 2 - source CyberKnown April 11. Cyber-tracker 12. Ukraine-Russia War

The most active CNSA on the battlefield was the collective Anonymous and its network of affiliates. The groups of hacktivists conducted multiple attacks against Russian and Belarus private businesses, critical infrastructure and government organizations. Most of the attacks aimed at destroying Russian propaganda, such as the hack of Russian Broadcaster and Radio station, and at breaching Russian private businesses to leak sensitive information and damage their operations.

Another group that is active since the beginning of the conflict is the so-called Ukraine IT Army, which is a collective of volunteers composed of cyber security experts called to action by the Ukraine government.

The Ukraine IT Army was involved in both defensive and offensive operations against Russia-linked targets. The collective of white hat hackers shared a list of targets, including critical infrastructure, government agencies, banks, and hosting providers.

The Ukraine IT Army was established in response to a call to action by Ukraine's Minister for Digital Transformation Mykhaylo Fedorov that invited cyber security experts to attack Russia.

Other threat actors involved in the cyber dispute are cybercrime gangs, in particular two ransomware gangs, the previously mentioned Conti and Stormous gang, that expressed their support to Russia. The presence of such kind of actors on the cybernetic battlefield should not be underestimated. These criminal organizations are known to be capable of gaining access to organizations worldwide to steal target's data and encrypt data stored on the victim's systems. These actors could support the activity of a nation-state actor by providing access to infrastructures previously compromised and pass stolen data.

Such active role of CNSA represents a novelty for a conflict and was debated at length by cybersecurity experts. Such actors could cause serious damages to the targeted infrastructures: thus, their support to military operations of one state could be precious. The presence of CNSA could also make it harder to attribute cyber-attacks. This is especially dangerous when dealing with the involvement of sophisticated and well-resourced cybercrime gangs. When dealing with attacks conducted by hacktivists the risk of potential infiltration by intelligence agencies is high. Intelligence agencies could influence with various means the operation of groups of hackers belonging to the collective or can impersonate them in false flag operations.

Impact of CNSAs on state socio-economic and geopolitical strength

Operations conducted by CNSA like Anonymous in the ongoing Russia-Ukraine conflict should also not be underestimated from an international legal and geopolitical point of view. In this scenario, a CNSA is moving war to a state, but a non-state actor is an entity with no specific physical territory and territorial sovereignty, with no clear identification of its components.

How would international law apply to such scenario? How could diplomacy or cyber- diplomacy help? Which are the possible actions of a state to bring peace.

It is worth studying or at least trying to ascertain the relevance of CNSA on a State socio-economic structure from different perspectives.

CNSA could have positive and negative influence for a State depending on certain key factors such as:

A. its level of cyber infrastructures (e.g. speed of data etc.),

B. its Judicial System and law enforcement capabilities in the cyberspace,

C. The set of values and ideals shared by its population.

Which is a kind of positive impact that CNSAs can have on a State socio-economic and geopolitical strength?

First of all, it is worth noting that, as mentioned above, CNSAs are quite often and mainly made of people with an above average level of cyber capabilities.

In a world where the use of internet and cyberspace is actually changing the way we think and act, and in a scenario where Metaverse and augmented reality will be redefining how we work and interact socially, fostering and creating the humus for proliferation of CNSAs, considering them as 'competence pools' could be a factor for enhancing a State's capability of competition in cyberspace and could also enhance the chances of defending its economic and social cybersphere (or enlarge its influence).

Secondly, if such CNSAs could and would act within the laws and regulations of the State, they could have a positive effect on the socio-economic life by acting, e.g., as whistle-blowers.

The negative influence that CNSAs can have on a single State are due to effects of their operations and their strategy. Some groups could operate damaging operations of critical infrastructures, private business and government organizations with a significant impact on the economy and social stability of a government.

Therefore, CNSAs can be considered as a double-edged sword from the point of view of effects. Consequently, it should be asked what the ideal set of conditions would be and what would be the single most important factor capable of influencing the set of rules of behaviour and moral code of CNSAs for a State.

It could be believed that is factor c) of the above-mentioned list should be the most important factor: a State where a clear set of values and ideals that are in line with the State's aims is the best condition for the positive interaction between CSNA and the State to the advantage of the latter.

From this perspective, it does not really matter if the set of values encompasses democratic ideals and / or a specific idea and concept of justice and rule of law. What is important is that such values are aligned with the State's aims.

Therefore, a dictatorial State whose aims are to foster capabilities of striking other countries in accordance with its necessities of the moment, would benefit from the presence of CNSAs sharing the values of National identity, love or respect for its leader (fear cannot be considered a value), and hate or despise for the target State or its values or actions.

By the same token a democratic State, whose CNSAs share the value of freedom and respect for individuals and freedom of speech and thought, could benefit from the presence and prosperity of such entities, enhancing its pool of cyber-competence, its capabilities to discover and pinpoint illegal behavior, to defend its cyberspace and socio-economic environment, and in certain cases, to strike back at attackers in a way not always allowed by rules: the way typical of hacktivists.

Another important factor influencing the presence and the development of CNSAs is the level of protection of individual privacy.

Democratic states should promote the conditions for creation of certain CNSAs with the goal of increasing the transparency of their operations and ensuring stability in a model of collective collaboration.

States that are not interested in collective participation for such purposes tend to stifle CNSAs, at least legitimate ones. They are more interested in using cyber nation-state groups and making them interact, in some scenarios, with cybercriminal organizations.

Conclusions

The operations of cyber non-state actors in cyberspace could have a severe impact for states, from cyber-attacks aimed at sabotage to online propaganda. The risks for states are increased by the possibility that other nations could use CNSA for their military and intelligence activities. Then, which are several policy options available to respond to such kind of operations attributed to a non-state actor?

A set of coherent actions could include:

- Requesting the host state to act against the hostile CNSA. It includes law enforcement and legal actions against the threat actors. It is essential to verify the due diligence[3] of the hosting country, its government is obliged to take measures to ensure its territories are not used by any threat actor to launch attacks against other states. The due diligence is very complex in the cyberspace due to the absence of borders;
- Promote diplomatic action in response to the CNSA's motivations.
- Supporting the target states in taking action against the malicious cyber operations;
- Sanctions;
- Cyber and conventional military response once attributed the attack to a certain CNSA and its infrastructure have been identified.

The above actions must be examined in an international context to avoid spillover and escalation of the cyber operations among states. In any case, the response to such attacks must be proportional. Sometimes CNSA could move the attacks from a country even without local government consent or knowledge. Additionally, any response to a cyber-attack should, of course, be proportional.

[3] Sico van der Meer from Clingendael Institute (2020) - How states could respond to non-state cyber-attackers

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies